WITS Technical Bulletin #39

Application Notes Affected: AN2005-001 version 1.3
AN2005-002 version 1.3
AN2007-001 version 1.3
Apps Notes Appendix A and B

and

WITS PSA Test Specification

Bulletin Reference: **TB0039 Iss 10**

Bulletin Type: **Clarification / Design Change**

Status: ~~**Circulated for comment / Rejected /**~~ **Accepted**

Date Issued: **16-Apr-12**

Authors: **B. Shephard**

1 Overview

This technical bulletin was initially used to discuss vulnerabilities of DNP3 Secure Authentication (SA) version 2 and changes for WITS-DNP3 to utilise SA version 5. This "Overview" section describes the roadmap of the SA document, the vulnerabilities of SA version 2 and considers the options available in SA version 5.

The vulnerabilities have been understood and the options have been agreed by the WITS PSAC, so the necessary changes to the WITS-DNP3 document pack are included in section 2.

1.1 DNP3 Secure Authentication versions

DNP3 SA was developed to add authentication and security layers to the basic DNP3 protocol standard. Security is not an absolute science and, as intruders become more sophisticated or potential vulnerabilities are detected, SA upgrades will be released to address these issues. It will not always be possible to maintain backwards compatibility. The SA roadmap to date has been:

- Version 1 (2007), internal document to the DNP3 Technical Committee.
- Version 2 (2008), first official SA publication.
- Version 3 (2010), internal document to the DNP3 Technical Committee
- Version 4 (2010), internal document to the DNP3 Technical Committee
- Version 5 (2011), latest SA publication, deprecating version 2.

In the above, the word "deprecating" is used to mean:

> Because SAv5 is not simply an extension of SAv2 but replaces some functionality of SAv2 with incompatible requirements, they cannot coexist in the specification and SAv5 must replace SAv2. Thus SAv2 becomes deprecated and is no longer recommended for use in **new** installations.

This means that a new vendor entering the market-place may have DNP3 support in his device with SA version 5. If WITS-DNP3 does not adopt SA version 5 then we may be closing the door on new vendors supplying WITS-DNP3 compliant devices.

It is recognized that it is not always practical or financially viable to update previously installed Field Device software with software compatible to a new SA standard. This may be the case with an update that corrects vulnerability in a topology not used in a given system, when a vendor has stopped manufacturing a given device, or simply when the user determines that the update is not warranted.

Thus the WITS PSAC Technical Team are recommending that it is **not** mandatory that WITS-DNP3 Field Devices deployed with SA version 2 need to be updated to support SA version 5. They do recommend that new Field Devices coming to the market-place implement the latest available version of DNP3 Secure Authentication.

WITS-DNP3 Master Station vendors should be aware that software supporting a current SA standard may not interoperate with Field Device software compatible to an older SA standard. It is the Master Station vendor's responsibility to verify the SA implementation levels of all Field Devices to which it will communicate and which employ SA. In some cases, this may require the Master Station software to support more than one SA standard and to enable the applicable one on a Field Device basis.

For this reason the WITS PSAC Technical Team are recommending that Master Stations certified for the WITS-DNP3 protocol version 2.0 are required to support the current SA version released from the DNP User Group. They may also be required to support older versions of SA to inter-operate with legacy Field Devices that implement older versions of SA. The Master Station "DNP3 device profile" will indicate which versions of SA they support.

1.2 Secure Authentication version 2 vulnerabilities

SA version 2 delivers authentication far superior to any security offered by the traditional SCADA protocols (proprietary and standard protocols). Using pre-shared keys the authentication algorithm allows a Master Station to determine that it is communicating with the expected Field Device and, likewise, allows the Field Device to determine that it is communicating with the expected Master Station i.e. neither Master Station nor Field Device are being spoofed.

However, during early SA version 2 implementations in WITS founder vendor devices it was found that the SA document did not explicitly state how devices were to cope with certain conditions:

a. What happens to session keys over a device restart?
b. The WITS requirement to make the function code "confirm" a critical function is not possible with SA version 2
c. Unsolicited responses could collide with a Master Station critical request, causing the request to time-out

WITS founder vendors identified these conditions and implemented solutions that ensured interoperability between their devices:

a. Session keys do not persist over a device restart (now stated in SA version 5)
b. The WITS requirement to make the function code "confirm" a critical function was changed to be optional. SA version 5 identifies those scenarios where "confirm" could not be critical and allows the function to be treated as a critical function in all other cases. Future versions of WITS-DNP3 should be able to re-introduce the user requirement that "confirm" is critical when it results in data being discarded from the Field Device.
c. Unsolicited responses could collide with a Master Station critical request, causing the request to time-out. WITS ignored this, assuming the Master Station would retry. SA version 5 caters for this condition by enhancing the structure of some of the security objects (thus making SA version 5 not compatible with SA version 2).

Non-founder vendor products implementing WITS-DNP3 version 1.1 or 1.2 know how to cope with these conditions because they were documented in TB#36.

So how vulnerable is a system that employs SA version 2?

1. Devices implementing SA version 2 did not differentiate between different error conditions:

   - authentication errors
   - configuration errors
   - general protocol errors
   - comms media errors (timeouts etc)

   This means that a device implementing SA version 2 may be sending many more error messages than one that implements SA version 5. The fact that SA version 5 throttles these error messages reduces the impact of some types of denial of service attacks.

2. A cyber attack on a device using SA version 2 will cause the devices to change their session keys after a number of authentication failures. Devices implementing SA version 5 will only change their session keys a "maximum number of times" after which they only change then at a configured "change interval". This means that a device implementing SA version 5 will throttle the number of session key changes, and thus reduce the impact of a denial of service attack which is sending continuous messages with bad authentication.

3. When using the protocol in unsolicited mode there are windows where there may be SA messages being sent to the Field Device at the same time as the Field Device is starting to send SA

messages to the Master Station. SA version 2 does not address this scenario so there are possibilities that one, or even both, of the SA message exchanges will fail. If the devices are configured with appropriate timeouts then the retry of the messages should succeed. SA version 5 addresses this scenario, changing the challenge scenario, which makes SA version 5 non-backwards compatible with SA version 2.

4. SA version 2 did not adequately document how the SA procedures in the devices should behave during restarts. This is one of the areas identified by the WITS founder vendors and an interoperable solution was developed by the vendors. SA version 5 now defines these procedures.
5. Devices implementing SA version 2 process unexpected messages, with the intent to try to re-establish normal comms as soon as possible. SA version 5 assumes that the unexpected message may be from an attacker and specifies the message must be discarded, thus reducing the impact of denial of service attacks from unexpected messages.

1.3 Secure Authentication version 2 / version 5 differences

- SA version 5 provides details that fix the vulnerabilities identified above.
- Devices implementing SA version 2 are required to keep some basic counts of authentication and protocol errors (statistics). When these exceed certain thresholds the communications session is closed and has to be re-established. SA version 2 has been analysed by a number of Cyber Security experts who have recommended that additional statistics be kept and that only certain error thresholds being exceeded shall cause the communications session to be closed. These additional statistics are detailed in SA version 5. Likewise, the changes about closing the communications session are documented in version 5. These changes improve the device's resilience to denial of service attacks.
- SA version 2 identifies a list of algorithms that can be used to encrypt certain parts of critical DNP3 messages. The evolving field of IT security has identified some new cryptographic algorithms. SA version 5 expands the list of algorithms that can be used and also deprecates the use of SHA-1, making support for SHA-256 mandatory (the new default).
- SA version 2 defined the DNP3 "file handling" function codes as being non-critical (i.e. optional). WITS-DNP3 devices wanted to secure their log files so the protocol defined file "open" and file "delete" functions as being critical. SA version 5 now defines all file handling function codes as critical.
- Finally, SA version 5 introduces the capability to change "user details" over the wire. This includes adding/deleting users, defining/changing user roles, and changing their update keys. In SA version 2 both the Mater Station and Field Device need to be locally configured with the pre-shared update key. If the key is ever compromised the user needs to visit both locations to locally configure a new key. With SA version 5 the key can be changed using the DNP3 communications session.

1.4 Secure Authentication version 5 options

1.4.1 Statistics

Support for the enhanced set of security statistics is mandatory. However, their reporting is always with flags but may optionally be with a time-tag. It is preferable for WITS-DNP3 devices to report security statistics with a time-tag and hence WITS-DNP3 should state this as mandatory requirement when SA version 5 or higher is implemented..

SA version 5 states that the Field Device **may** report these statistic objects to a Master Station other than that involved with the authentication. In the WITS environment we only have the one Master

Station and hence this statement is to be interpreted as statistic objects will be reported to the Master Station involved with the authentication.

1.4.2 Remote 'update key' changes

The support for remote update key changes is optional in the DNP3 specification. The WITS PSAC Technical Team recommends that it is to be optional in WITS-DNP3 version 2.0. The DNP3 Device Profile will show if support for remote update key changes is available in a device that implements SA version 5. When remote update key change is supported it shall be supported using symmetric cryptography. The WITS PSAC Technical Team do not recommend implementing the optional asymmetric cryptography methods in WITS-DNP3 compliant devices. However, devices may choose to do so – in which case this support is to be detailed in the DNP3 Device Profile.

SA version 5 contains a lot of functionality associated with "Role Based Access Control (RBAC)" i.e. the management of "users", utilising a model in the Field Device of many users, each with their own roles, areas of responsibility, and each with their own update key. The SA version 5 document shows how all of this user information is obtained from a trusted third party known as an "Authority[1]", which is an entity other than the Master Station. The Master Station has to communicate with the Authority – but how this is done is outside of the scope of SA version 5. Likewise, the Field Device has to be able to interpret the information from the Authority and validate it, meaning the Field Device needs to know about users, roles and areas of responsibility.

WITS Field Devices do not have a complex model for users. We have a single user (the Master Station) and we delegate the functions of RBAC to the Master Station. If a WITS device implements remote update key changes then we must assume that the DNP3 device driver implemented in the Master Station can securely obtain the minimum set of information needed to implement the function:

- An encrypted new "update key", encrypted using the "Authority Certification Key" which it configurable into the Field Device

Using symmetric cryptography the Master Station exchanges objects with the Field Device, these objects relating to the user "Common" (the DNP3 standard for the generic comms session between the Master Station and the Field device). WITS-DNP3 version 2.0 will define a private "role" which is suitable for use by WITS devices (i.e. a role that enables unlimited functionality).

Master Stations may choose to implement a more complex RBAC model as detailed in the DNP3 documentation – but this is outside of the scope of WITS-DNP3.

Similarly, Field Devices may choose to support a more complex RBAC model as detailed in the DNP3 documentation – but this is outside of the scope of WITS-DNP3.

1.5 Summary:

- SA version 2 is the security algorithm specified as part of the WITS-DNP3 protocol in versions up to and including 1.2.

---

[1] Extracted from DNP3 Secure Authentication version 5 – "The authority is necessary to certify that users are to be added or removed, or that their roles should be changed. It separates the functions of secure communications from the functions of managing Update Keys and users. No particular user of a master or outstation shall be trusted with the capability to add or remove users from an outstation, or to change the actions a user is permitted to perform. That function must be performed by a central authority whose scope is the entire organization. The authority may or may not be what is commonly known as a Certificate Authority, although it performs a similar function."

- WITS-DNP3 version 2.0 will recommend support for the current SA version available from the DNP3 User Group in the Master Station, with optional support for earlier versions to enable the Master Station to inter-operate with legacy Field Devices. The DNP3 Device Profile will detail which version(s) of SA are supported in the device and any optional features.
- Existing WITS-DNP3 Field Devices deployed with SA version 2 do not need to be migrated to the current SA version available from the DNP3 User Group
- WITS-DNP3 will not mandate the support for remote update key changes
- It is the user's responsibility to ensure that his Master Station is able to support the SA versions and functions implemented in the Field Devices that he intends to use.

The above discussion was summarised on the single page (shown overleaf) and discussed and agreed amongst the PSAC members during their February 2012 teleconference. Note that colours shown on the next page do not reflect the use of colours for adding/deleting text that is used in section 2 of this Technical Bulletin.

Security Requirements for WITS Compliant Devices

The WITS-DNP3 protocol standard relies on the DNP3 Secure Authentication procedures to achieve its security goals. DNP3 Secure Authentication provides functions and data objects that permit devices to authenticate DNP3 communication messages by verifying the source of the message and that the message was transmitted without modification.

Over time, new security threats will be discovered and new methods devised to compromise existing techniques. As new techniques are developed that expose or exploit security flaws, new measures need to be developed to address those changes and maintain system security. This is an on-going cycle that never ends and new versions of DNP3 Secure Authentication will be released from time to time as required to address the changes in the evolving threat landscape.

The following summarises the key features available with the currently published versions of DNP3 Secure Authentication and their relevance to WITS compliant devices.

	DNP3 SA version 2	DNP3 SA version 5	WITS requirement
Message authentication	✓	✓	✓
"User" model: - multiple users	✓	✓	single user
- remotely add / delete users	✘	✓	✘
- remotely change user's roles	✘	✓	✘
- remotely change user's time to live	✘	✓	✘
- remotely change user's update key	✘	✓	optional
- obtain user details from PKI (X.509) certificate	✘	✓	✘
Maintain security statistics	✘	✓	optional
Improved resilience to denial of service attacks	n/a	✓	optional
Uses the latest cryptography algorithms	n/a	✓	Optional

From this we can see that WITS-DNP3 security requirements do not mandate the use of DNP3 Secure Authentication version 5. However, devices implementing the latest version of DNP3 Secure Authentication may offer added value to the user. It is the user's responsibility to ensure that the devices he intends to use are inter-operable with the versions of Secure Authentication in the devices.

The WITS PSAC are endorsing the recommendations from the DNP User Group:

> **It is highly recommended that outstations be deployed with the latest version of Secure Authentication as published by the DNP Users Group. However, in order to be interoperable, new outstations being deployed in a system may be required to implement a specific version of Secure Authentication, as supported by the master station.**
>
> **Similarly, it is highly recommended that master stations be deployed with the latest version of Secure Authentication as published by the DNP Users Group. It may be advantageous for new master station deployments to implement several versions of Secure Authentication in order to operate with outstations already deployed in the field.**

Devices that implement DNP3 Secure Authentication have security far superior to any security offered by the traditional SCADA protocols (proprietary and standard protocols).

NB. In section 2 onwards, text that is shown in red represents words to be removed from the application notes and text in blue represents words to be inserted into the notes.

2 Changes to the Application Notes

2.1 Release pack header pages etc

Change front page as shown:

Release 34
June 2011April 2012
WITS-DNP3 Protocol Version 1.22.0

Change second page as shown:

Release 34 document revision details:

1. Application Notes (this document)

Note	Title	Revision
AN2005-001	WITS DNP3 Usage Overview	1.3 4
AN2005-002	WITS Interoperability	1.3 4
AN2005-003	WITS Use of Object Group 0	1.1
AN2005-004	WITS Data Logging	1.3
AN2005-005	WITS Data Sets	1.3
AN2005-006	WITS Incremental Configuration	1.3
AN2007-001	WITS Detailed Interoperability	1.3 4

2. Compliance Testing (separate documents)

Title	Revision
WITS Compliance Manual	2.3
WITS Supplement to Level 2 Test Procedures	0.5

3. WITS Device Profile (separate XML package)

Title	Revision
WITS Device Profile XML Schema	1.4
WITS Device Profile XSLT Style sheet	1.4
Example WITS Device Profile XML Instance File	1.4
WITS Device Profile document template	1.4

Change all footers as shown:

WITS Application Notes ***WITS-DNP3 Protocol Version 1.22.0***
June 2011 Release 3April 2012 Release 4

2.2 AN2005-001

Change front page as shown:

Revision 1.34

June 2011April 2012

Change "Change History" as shown:

Date	Revision	WITS-DNP3 Version	Details
May 2010	1.0	1.0	Incorporating all details up to and including TB #32.
June 7 2010	1.1	1.0	WITS Release 1.0 uses DNP3 secure authentication version 2.00. Version 3.00 will be used in a future release later in 2010.
December 2010	1.2	1.1	Correct spelling of "Archives"iin table 2-1. Update (throughout the notes) to WITS-DNP3 version 1.1
June 2011	1.3	1.2	Rename "Limit Profiles" to "Profiles" and introduce the term "Profile Control Value". Add the term "Derived Point" to the glossary.
April 2012	1.4	2.0	Introduce DNP3 Secure Authentication version 5.

Update section 2.2.4 as shown:

2.2.4 Security

The DNP3 Ssecure Aauthentication (SA) standard has been adopted by WITS. WITS-DNP3 protocol versions prior to version 2.0 implemented SA version 2, as defined by the DNP3 volume 2 secure authentication supplement (version 2.00 DNP3 Vol2-Supp1 Secure Authentication v2 2008-07-31.pdf).

In 2011 the DNP User Group published SA version 5 (DNP3 Vol2-Supp1 Secure Authentication v5 2011-11-08.pdf) and deprecated SA version 2. The "deprecation" of SA version 2 means that its use is discouraged in new devices but may exist in current implementations. SA version 5 provides authentication with:

- Improved resilience to denial of service attacks
- Improved collection of potential cyber attack statistics
- The option for remote "update key" changes

B**ecause** the adoption of SA version 5 is not mandatory (but recommended by both the DNP User Group and the WITS PSA Committee) devices implementing WITS-DNP3 version 2.0 shall:

- If a Master Station, support both Secure Authentication version 2 and version 5 (to ensure interoperability with new Field Devices that choose to implement Secure Authentication version 5). The support for remote update key change is required.
- If a new Field Device, preferably support Secure Authentication version 5. The support for remote update key change is optional.
- If a legacy Field Device, optionally upgrade to support Secure Authentication version 5. The upgrade to support remote update key change is optional.

The implementation of security is discussed in further detail within [AN2005-002 and AN2007-001].

2.3 AN2005-002

Change front page as shown:

Revision 1.34

June 2011April 2012

Change "Change History" as shown:

Date	Revision	WITS-DNP3 Version	Details
May 2010	1.0	1.0	Incorporating all details up to and including TB #32.
June 7 2010	1.1	1.0	Correction to data set name in 2.6.3
December 2010	1.2	1.1	Modified change history table layout
June 2011	1.3	1.2	Rename "Limit Profiles" to "Profiles" and introduce the term "Profile Control Value". Added new section at end of part 2 "Data Derivation". Added section about "Backwards Compatibility".
April 2012	1.4	2.0	Introduce DNP3 Secure Authentication version 5.

Update section 2.6.1 as shown:

2.6.1 Security

A joint IEC60870 / DNP3 group has been setup to address a standard for embedding authentication into the protocols. Experts from a number of standardisation bodies (including the IEC, IEEE, DNP3 Technical Committee) have collaborated to develop standards for implementing security features into SCADA protocols. Details of these standards can be found in IEC62351. The DNP3 group Technical Committee has created a document: DNP3Spec-V2-Sup1-SecureAuthentication-20080731.pdf DNP3 Vol2-Supp1 Secure Authentication v2 2008-07-31.pdf. This standard has been adopted by WITS in the WITS-DNP3 protocol versions 1.1 and 1.2. The document is intended to deliver the following:

- A mechanism for authenticating Field Devices.
- A mechanism for implementing message sequencing.

A mechanism for updating the authentication keys has been defined in a more recent version of the DNP3 standard (DNP3Spec-V2-Sup1-SecureAuthentication-20100317.pdf) and will be adopted by a future version of the WITS standard. remote changing of the pre-shared "update" keys has been developed and, with other security enhancements, is now documented as Secure Authentication version 5 (see DNP3 Vol2-Supp1 Secure Authentication v5 2011-11-08.pdf). Optional support for Secure Authentication version 5 is now adopted in the WITS-DNP3 protocol version 2.0.

Master Stations that implement WITS-DNP3 version 2.0 may be required to communicate with legacy Field Devices that implement Secure Authentication version 2. WITS compliant Master Stations are therefore required to support both version 2 and version 5 Secure Authentication (and any future versions of Secure Authentication as they are released from the DNP User Group).

Technical details of the implementation of Secure Authentication in WITS-DNP3 can be found in section 4.10 of AN2007-001.

2.4 AN2007-001

Change front page as shown:

Revision 1.34

June 2011April 2012

Change "Change History" as shown:

Date	Revision	WITS-DNP3 Version	Details
May 2010	1.0	1.0	Incorporating all details up to and including TB #32.
June 7 2010	1.1	1.0	Corrected details in table 4-1, records 1003 & 1004
December 2010	1.2	1.1	Corrected flow directions in figures in scenarios G (flow 4) and scenario H (flow 3). Clarified and added notes to 2.3.1 Added new notes to 3.1.1 and 4.3.1 Added new para (para 3) to section 3.1.2 Added para to 4.8 Corrected 4.3.2 and 4.7.2 describing "restart" behaviour
June 2011	1.3	1.2	Rename "Limit Profiles" to "Profiles" and introduce the term "Profile Control Value". Introduce HCDS bit "IC parameter value changed".
April 2012	1.4	2.0	Introduce DNP3 Secure Authentication version 5.

Add new section 4.10 as shown:

4.10 Implementing DNP3 Secure Authentication (SA)

DNP3 SA was developed to add authentication and security layers to the basic DNP3 protocol standard. Security is not an absolute science and, as intruders become more sophisticated or potential vulnerabilities are detected, SA upgrades will be released to address these issues.

It will not always be possible to maintain backwards compatibility and so Master Stations (compliant to WITS-DNP3 version 2.0 or higher) shall be able to communicate with Field Devices that may be implementing different versions of SA. It is expected that the Master Station will be configurable to use a specific version of SA for each individual Field Device.

Implementations of SA version 2 are as defined in the DNP3 document "DNP3 Vol2-Supp1 Secure Authentication v2 2008-07-31.pdf" with the additional requirement of the WITS "critical functions" as shown in appendix B of these notes.

Implementations of SA version 5 are as defined in the DNP3 Specification "DNP3 Vol2-Supp1 Secure Authentication v5 2011-11-08.pdf" with the additional requirement of the WITS "critical functions" as shown in appendix B of these notes. However, for devices implementing SA version 5 there are a number of options as detailed in the following sections.

4.10.1 Master Stations and trusted third parties

The DNP3 specification of SA version 5 uses the two terms:

- Authority
  A trusted third party, used to certify that users may be added or removed, or that their roles should be changed.
- Master Station
  Any entity that issues requests to gather data or perform controls using DNP3.

When performing remote update key changes there is a requirement for the Master Station to interface to the Authority. In the UK WMO telemetry systems the DNP3 term Master Station would be referring to the WITS-DNP3 protocol driver. In order to implement remote update key changes the system therefore needs a trusted entity to issue the new update key in an encrypted form to the protocol driver. The remote Field Device needs knowledge of the Authority encryption key to be able to decrypt the new update key.

WITS-DNP3 does not mandate the support for the complete role based access control model as defined in the DNP3 Specification. WITS-DNP3 expects that most of the role based access control is implemented in components of the Master Station telemetry system. The UK WMO telemetry systems may therefore consider the Authority as anything from a conventional Certification Authority (issuing digital certificates) to a simple secure application (as a component of the telemetry system) which merely takes a new update key from the Master Station and returns it encrypted with the Authority's key.

4.10.2 SA version 5 in the Master Station

If the Master Station supports SA version 5 or higher it shall support the complete range of statistical points listed in table 7-6 of clause 7.5.2.2 of the DNP3 Specification. It shall support these being reported using any of the DNP3 objects from group 121 variation 1 or group 122 variations 1 or 2.

If the Master Station supports SA version 5 or higher it shall implement the improved resilience to denial of service attacks as detailed in clause 7.5 of the DNP3 Specification.

If the Master Station supports SA version 5 or higher it shall optionally support remote changing of Field Device update keys using symmetric cryptography methods.

When using symmetric cryptography the DNP3 objects shall be populated with:

- username - set as "Common"
- role – set to the "SINGLEUSER" role, value 32768. Note that role is under discussion by the DNP Technical Committee and is expected to be defined in an update to the DNP Specification.
- expiry interval – set typically to 1095 days (3 years)

4.10.3 SA version 5 in a Field Device

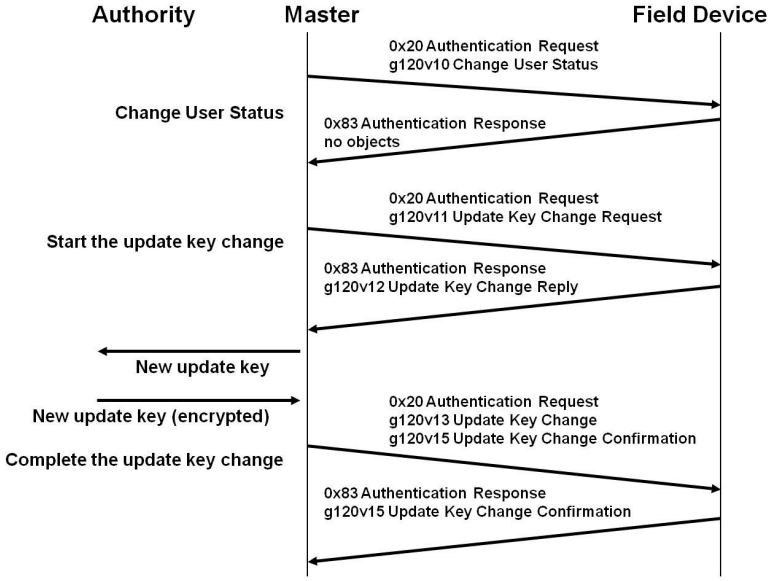
A Field Device shall support the complete range of statistical points listed in table 7-6 of clause 7.5.2.2 of the DNP3 Specification. It shall preferably report these using the DNP3 objects with group 121 variation 1 and with group 122 variation 2 (or alternatively with group 121 variation 1 and with group 122 variation 1).

If a Field Device supports SA version 5 or higher it shall optionally support remote changing of update keys using symmetric cryptography methods.

When supporting symmetric cryptography it shall support the objects populated as detailed in section 4.10.1.above.

4.10.4 Remote update key change message exchanges

The following is an informative section showing the message exchanges used to perform a remote update key change, using symmetric cryptography.



1. The Master Station sends a “change user status” request (g120v10) to the Field Device. The message requests an operation of “Change” and has other elements containing:
   - key change method, to be set to the symmetric cryptography default of:
     <4> := Symmetric AES-256 / SHA-256-HMAC
   - user name, set to “Common” to show this is the common user for the Master Station / Field Device session
   - user role (see details in 4.10.2 above)
   - time to expire, which the related IEC62351-8 standard defines as a maximum value of 3 years
2. The Field Device responds with a null response.
3. The Master Station sends an “update key change” request (g120v11) to the Field Device. The message contains some of the data elements from the g120v10 request.
4. The Field Device responds with an “update key change” reply (g120v12).
5. The Master Station defines a new update key which is then passed to the Authority.
6. The Authority encrypts the update key with the Authority’s “Certification Key” which has previously been shared between the Authority and all Field Devices.

7. The Master Station sends two objects in one request:
   - “update key change” (g120v13)
   - “update key confirmation” (g120v15)
   The first of these contains the new, encrypted, update key.
   The second contains a Message Authentication Code (MAC) that has been calculated using the new update key.
8. The Field Device responds with an “update key confirmation” reply (g120v15). The reply contains a MAC calculated using the new update key.

2.5 Apps Notes appendix A

Add to the table as shown (note that in the final document release the table entries will be shown as white text on a magenta background):

DNP3 OBJECT GROUP & VARIATION			REQUEST (master may issue, field device must parse)		RESPONSE (field device may issue, master must parse)	
Object Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
120	10	Change User Status	32 (auth request)	5B (free format)		
120	11	Update Key Change Request	32 (auth request)	5B (free format)		
120	12	Update Key Change Reply			131 (auth resp)	5B (free format)
120	13	Update Key Change	32 (auth request)	5B (free format)		
120	15	Update Key Change Confirmation	32 (auth request)	5B (free format)	131 (auth resp)	5B (free format)
121	1	Security statistic - 32-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all) 17, 28 (index)	129 (response)	00, 01 (start-stop) 17, 28 (index)
122	1	Security statistic event - 32-bit with flag	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response)	17, 28 (index)
122	1	Security statistic event - 32-bit with flag			130 (unsol resp)	17, 28 (index)
122	2	Security statistic event - 32-bit with flag and time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response)	17, 28 (index)
122	2	Security statistic event - 32-bit with flag and time			130 (unsol resp)	17, 28 (index)

2.6 Apps Notes appendix B

Change the table as shown:

Function Code		Description	Critical (WITS-DNP3 v1.1 & v1.2)	Critical (WITS-DNP3 v2.0)
Decimal	Hex			
0	0x00	Confirm	optional	MANDATORY
1	0x01	Read	optional	optional
2	0x02	Write	MANDATORY	MANDATORY
3	0x03	Select	MANDATORY	MANDATORY

Function Code		Description	Critical (WITS-DNP3 v1.1 & v1.2)	Critical (WITS-DNP3 v2.0)
Decimal	Hex			
4	0x04	Operate	MANDATORY	MANDATORY
5	0x05	Direct Operate	MANDATORY	MANDATORY
6	0x06	Direct Operate – No Acknowledgement	MANDATORY	MANDATORY
7	0x07	Immediate Freeze	optional	optional
8	0x08	Immediate Freeze – No Acknowledgement	optional	optional
9	0x09	Freeze-and-Clear	optional	optional
10	0x0A	Freeze-and-Clear – No Acknowledgement	optional	optional
11	0x0B	Freeze-at-Time	optional	optional
12	0x0C	Freeze-at-Time – No Acknowledgement	optional	optional
13	0x0D	Cold Restart	MANDATORY	MANDATORY
14	0x0E	Warm Restart	MANDATORY	MANDATORY
15	0x0F	Initialize Data (obsolete)	optional	optional
16	0x10	Initialize Application	MANDATORY	MANDATORY
17	0x11	Start Application	MANDATORY	MANDATORY
18	0x12	Stop Application	MANDATORY	MANDATORY
19	0x13	Save Configuration (deprecated)	optional	optional
20	0x14	Enable Unsolicited Responses	MANDATORY	MANDATORY
21	0x15	Disable Unsolicited Responses	MANDATORY	MANDATORY
22	0x16	Assign Class	MANDATORY	MANDATORY
23	0x17	Delay Measurement	optional	optional
24	0x18	Record Current Time	MANDATORY	MANDATORY
25	0x19	Open File	MANDATORY	MANDATORY
26	0x1A	Close File	optional	MANDATORY
27	0x1B	Delete File	MANDATORY	MANDATORY
28	0x1C	Get File Information	optional	MANDATORY
29	0x1D	Authenticate File	MANDATORY	MANDATORY
30	0x1E	Abort File	optional	MANDATORY
31	0x1F	Activate Configuration	MANDATORY	MANDATORY
32	0x20	Authentication Request (new)	Not applicable	Not applicable
33	0x21	Authentication Request – No Ack (new)	Not applicable	Not applicable
129	0x81	Response	optional	optional
130	0x82	Unsolicited Response	optional	optional
131	0x83	Authentication Response (new)	Not applicable	Not applicable

3 Changes to the WITS PSA Test Specification

The publication of DNP3 Secure Authentication version 5 changes the table of critical function codes which has an impact on the function codes that WITS define as critical. Changes are thus needed to the WITS PSA Test Specification, the changes detailed below.

Testing of Secure Authentication procedures is covered by a test specification being developed by the DNP3 User Group.

3.1 Changes to the WITS-DNP3 Test Specification Rev 1.2

Change the title page as shown:

Revision 1.22.0

June 2011April 2012

and put the new date and version in the document footers.

Add to the Change History as shown:

Date	Revision	WITS-DNP3 Version	Details
May 2011	1.1	1.1	First release for WITS-DNP3 protocol version 1.1.
June 2011	1.2	1.2	Updated for protocol version 1.2 and expanded testing to improve coverage of selected areas.
April 2012	2.0	2.0	Updated to reflect the publication of DNP3 Secure Authentication version 5.

Change the copyright notice as shown (and also update the copyright date in the document footers):

Copyright © WITS Protocol Standards Association 20112 All rights reserved

3.1.1 Section 2.12.1, application note references

Add a new reference to the table as shown:

Application Note	Version	Section
AN2005-001	1.3	2.2.4 Security
AN2005-002	1.3	2.6.1 Security
AN2007-001	1.4	4.10 Implementing DNP3 Secure Authentication (SA)

3.1.2 Section 2.12.2, critical functions

Add a new reference to the table as shown:

Application Note	Version	Section
AN2005-001	1.3	2.2.4 Security
AN2005-002	1.3	2.6.1 Security
AN2007-001	1.4	4.10 Implementing DNP3 Secure Authentication (SA)
Appendix B		DNP3 Authentication – WITS Critical Functions

In the table listing critical functions, change the entry for “direct operate no ack” as shown and remove the red fill. i.e. change

6	0x06	Direct Operate – No Acknowledgement	

to

6	0x06	Direct Operate – No Acknowledgement	2.12.2.3

Extend the test number 2.12.2.3 as shown:

3.1.2.1	Analogue/Binary Output test Initiate a communications session between the Field Device and Master Station. From the Master Station: Perform a Select, Operate, and Direct Operate and Direct Operate No Ack on an Analogue/Binary Output point.	Authentication should have been exchanged for each of the following functions: Select (Function 3) Operate (Function 4) Direct Operate (Function 5) Direct Operate No Ack (Function 6)		